Acceso independiente

Guía de inicio rápido

V1.0.1

V1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico de Access Standalone (en lo sucesivo, "autónomo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
PELIGRO	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un riesgo potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Marzo de 2020
V1.0.1	Agregue la altura de instalación recomendada.	Junio de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual. El manual se
- actualizará de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la
- descripción de funciones y operaciones, o

errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o

- pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado de la unidad autónoma, la prevención de peligros y la prevención de daños a la propiedad. Lea atentamente estos contenidos antes de utilizar el dispositivo independiente, cúmplalos al utilizarlos y guárdelos bien para futuras consultas.

Requisito de operación

- No coloque ni instale la unidad independiente en un lugar expuesto a la luz solar o cerca de una fuente de calor.

- Mantenga la unidad independiente alejada de la humedad, el polvo o el hollín.
- Mantenga el autónomo instalado horizontalmente en el lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre el autónomo, y asegúrese de que no haya ningún objeto lleno de líquido sobre el autónomo para evitar que el líquido fluya hacia el autónomo.
- Instale el autónomo en un lugar bien ventilado y no bloquee la ventilación del autónomo.

- Opere el autónomo dentro del rango nominal de entrada y salida de energía. No desarme el
- independiente.
- Transporte, use y almacene el dispositivo independiente en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Al
- reemplazar la batería, asegúrese de utilizar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.

- Utilice el adaptador de corriente que se proporciona con la unidad independiente; de lo contrario, podría provocar lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con los requisitos del estándar de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.

- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1 Dimensiones y componentes

Figura 1-1 Vista frontal (mm [pulgadas])

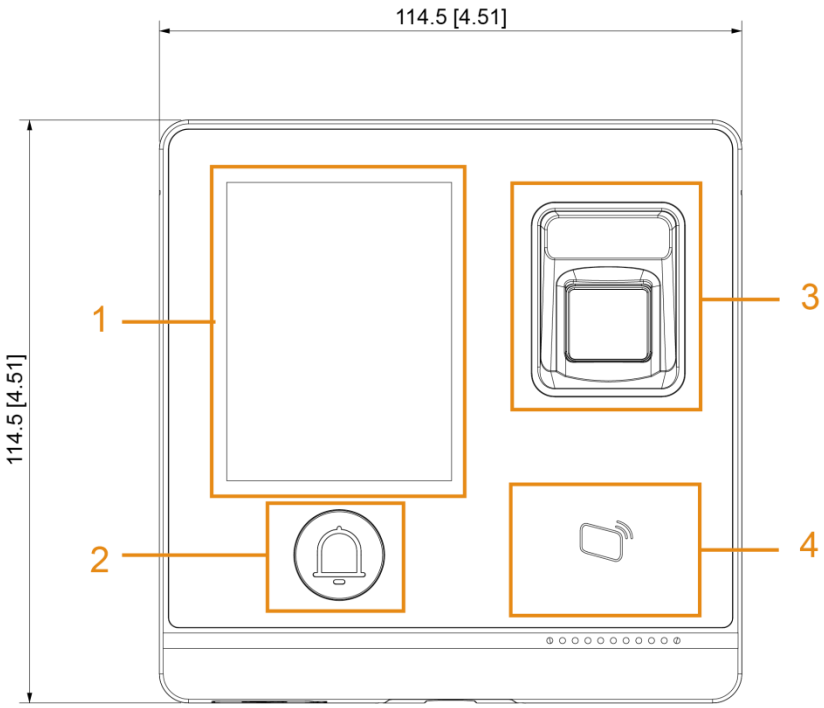


Figura 1-2 Vista posterior (mm [pulgadas])

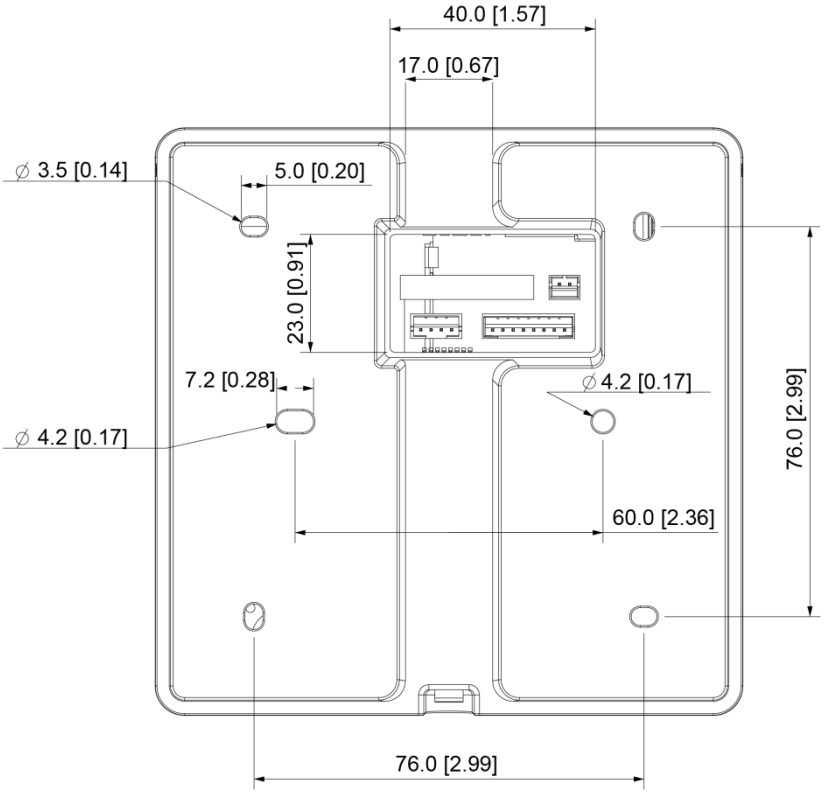


Figura 1-3 Vista lateral e inferior (mm [pulgadas])

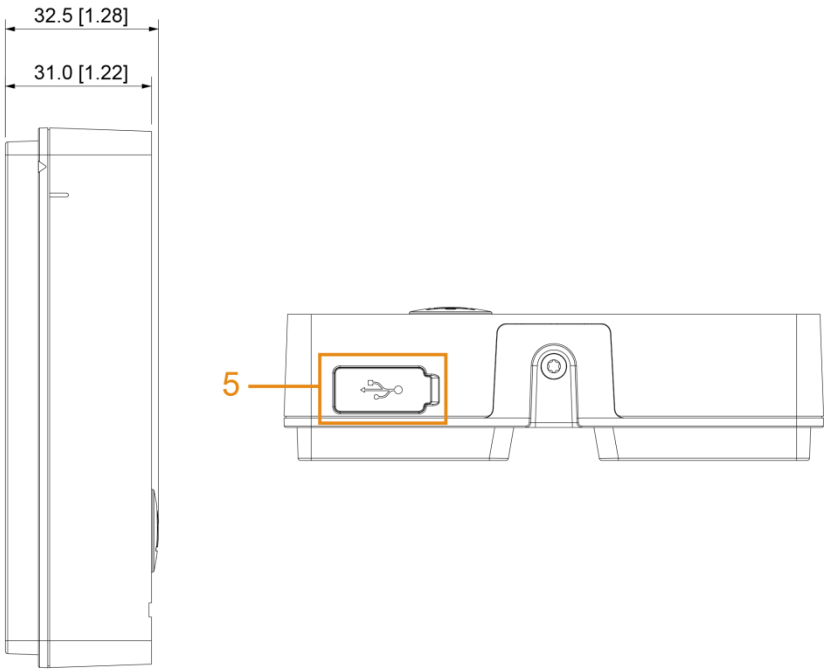


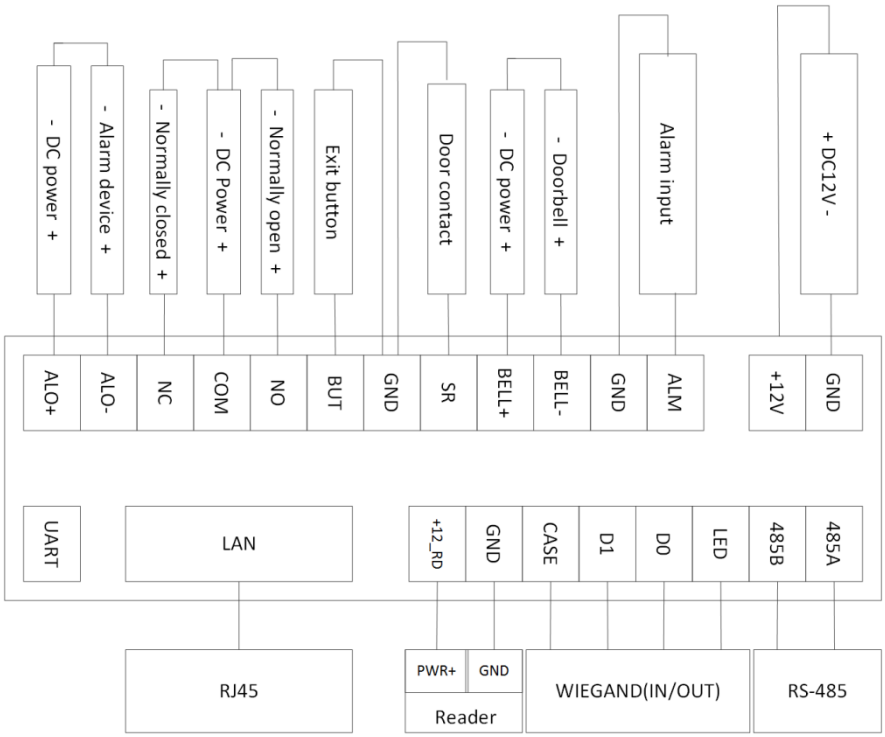
Tabla 1-1 Descripción de los componentes

No.	Nombre
1	Área de VA
2	Botón de timbre
3	Sensor de huellas dactilares
4	Área de deslizamiento de tarjetas
5	Puerto USB

2 Instalación

2.1 Conexión de cable

Figura 2-1 Conexión de cables



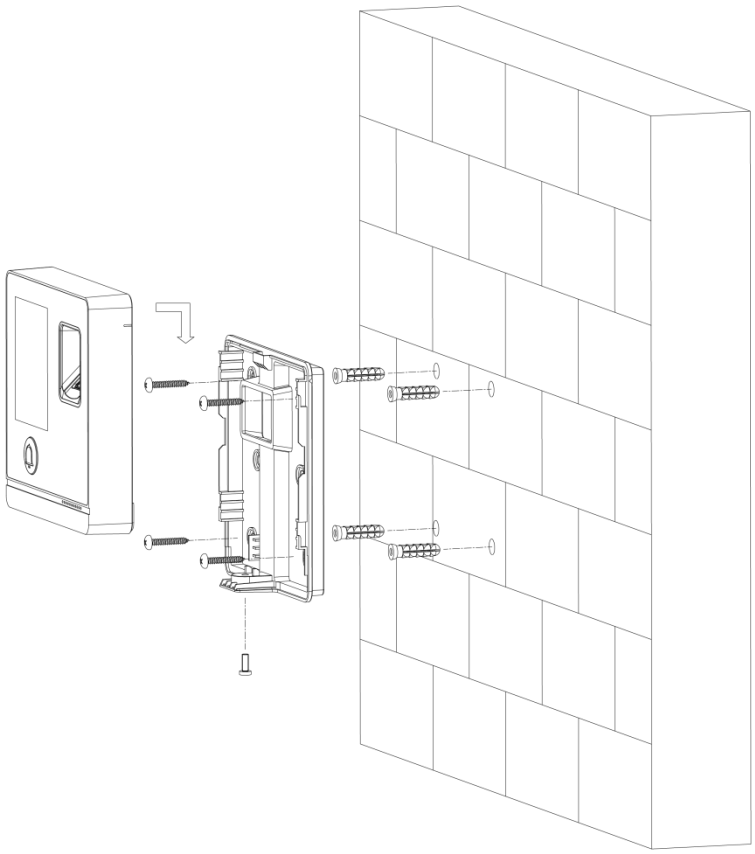
2.2 Instalación del dispositivo

La altura de instalación recomendada es de 1,4 a 1,6 metros.

El independiente admite la instalación en superficie y la instalación oculta.

Instalación en superficie

Figura 2-2 Instalación en superficie



Procedimiento de instalación

Paso 1 Pegue el mapa de instalación en la pared y luego taladre los orificios de acuerdo con las posiciones mapa.

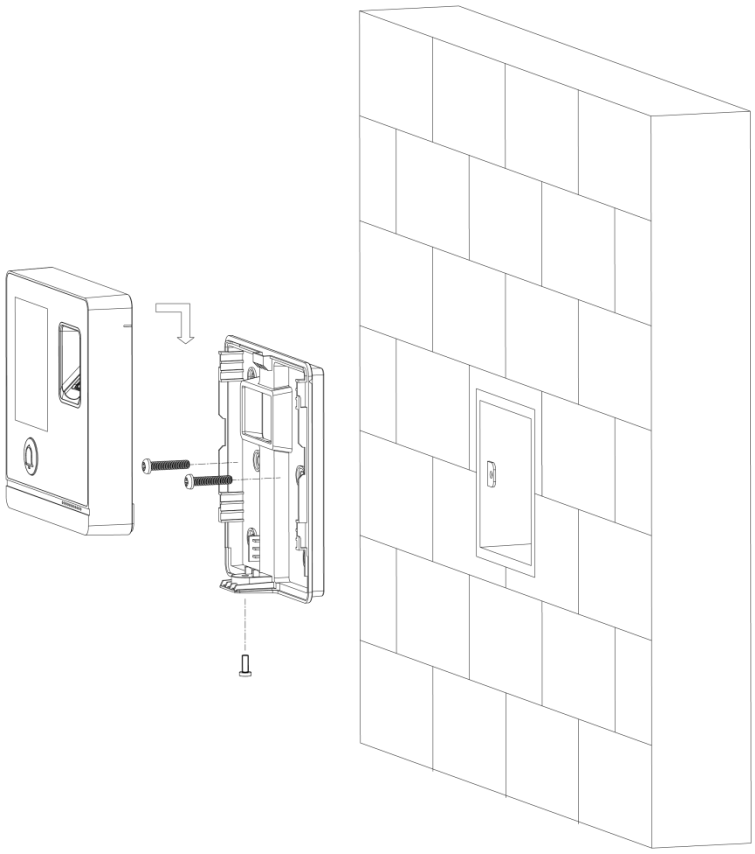
Paso 2 Inserte el perno de expansión en los orificios de instalación.

Paso 3 Fije la cubierta trasera a la pared con tornillos autorroscantes.

Paso 4 Coloque tornillos de máquina a través del orificio inferior; bloquee la cubierta frontal en la cubierta trasera.

Instalación oculta

Figura 2-3 Instalación oculta



Procedimiento de instalación

Paso 1 Pase los cables por la salida.

Paso 2 Fije la cubierta trasera en la caja montada con tornillos.

Paso 3 Fije los cables y abroche la cubierta frontal a la cubierta posterior.

3 Operación del sistema

3.1 Inicialización

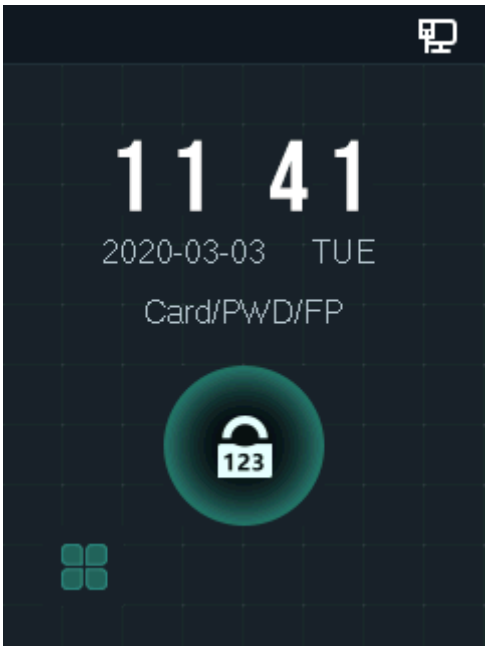
La contraseña de administrador y un correo electrónico deben establecerse la primera vez que se enciende el modo autónomo; de lo contrario, no se puede utilizar el independiente.

Figura 3-1 Inicialización

- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el administrador olvida la contraseña de administrador.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &).

Una vez completada la inicialización, se muestra la interfaz de espera.

Figura 3-2 Interfaz de espera

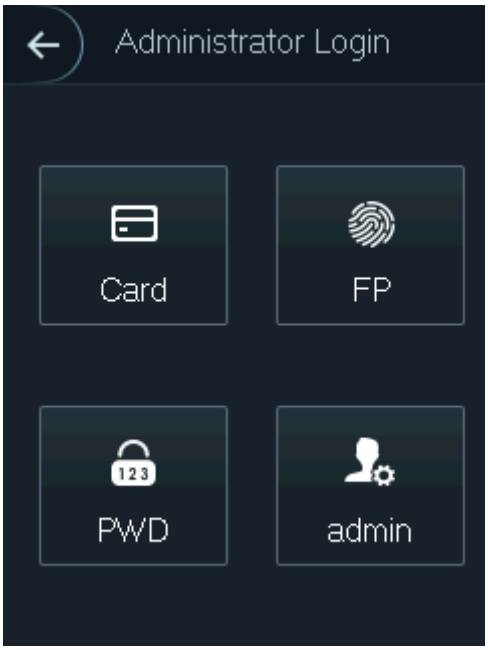


3.2 Agregar nuevos usuarios

Puede agregar nuevos usuarios ingresando sus ID de usuario, nombres, importando huellas digitales, contraseñas, seleccionando sus niveles de usuario y más.

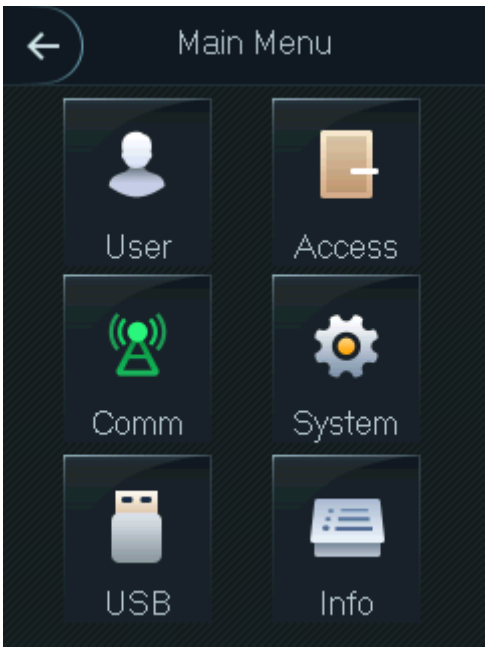
Paso 1 toque  en la interfaz de espera.

Figura 3-3 Inicio de sesión de administrador



Paso 2 Seleccione un método de entrada al menú principal.

Figura 3-4 Menú principal

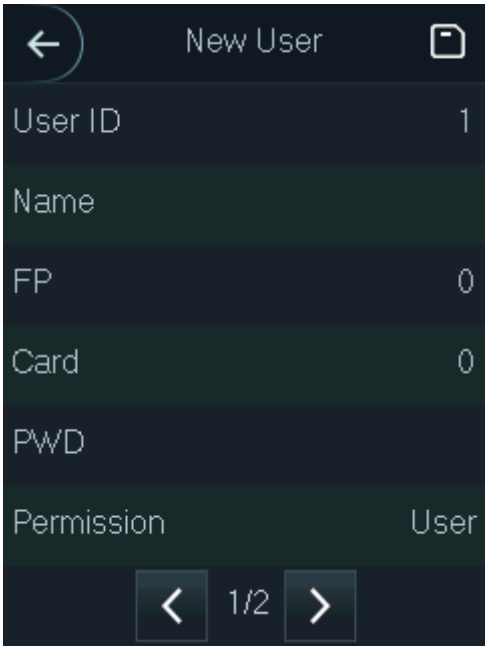


Paso 3 Toque 

y luego toque  .

La siguiente figura es solo de referencia y prevalecerá la interfaz real.

Figura 3-5 Nuevo usuario



Paso 4 Configure los parámetros en la interfaz.

Tabla 3-1 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede ingresar ID de usuario. Los ID constan de 18 caracteres (incluidos números y letras, pero no caracteres especiales) y cada ID es único.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Registro de huellas dactilares. Registre las huellas digitales del usuario. Registro de
Tarjeta	tarjeta. Registre la información de la tarjeta.
PWD	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de identificación es 8. Establezca el permiso del
Permiso	usuario: **Usuario** o **Administración.** • Usuario: **Usuario** solo tiene permiso para abrir la puerta. Administración: **Administración** tiene permiso para • desbloquear la puerta y configurar los parámetros.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta. Para conocer la configuración detallada del período, consulte el manual de configuración.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede abrir la puerta. Para conocer la configuración detallada del plan de vacaciones, consulte el manual de configuración.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.

Tipo de usuario	• General: los usuarios generales pueden desbloquear la puerta normalmente. • Restringido: cuando los usuarios de la lista negra desbloquean la puerta, el personal de servicio recibirá un aviso. • Invitado: los invitados pueden abrir la puerta en determinados momentos en determinados períodos. Una vez que superan los tiempos y períodos máximos, no pueden volver a desbloquear la puerta. • Patrulla: los usuarios que patrullan pueden hacer un seguimiento de su asistencia, pero no tienen autoridad de desbloqueo. • VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Otro: cuando usuarios • especiales (como personas discapacitadas y embarazadas) desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
Usar tiempo	Cuando el nivel de usuario es **Invitado,** puede establecer el número máximo de veces que el huésped puede abrir la puerta.

Paso 5 Una vez que haya configurado todos los parámetros, toque  para guardar la configuración.

4 Operación web

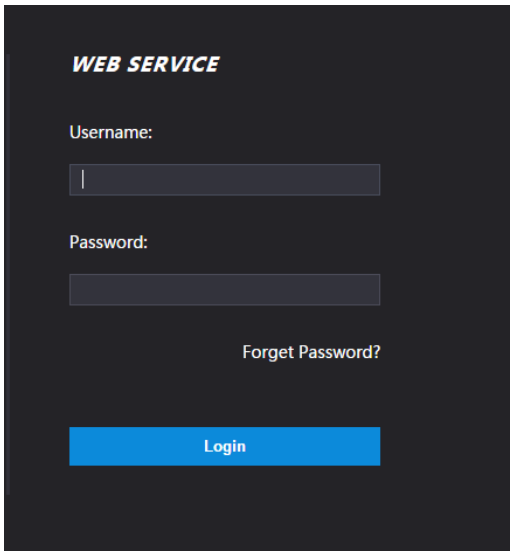
El autónomo se puede configurar y operar en la web. A través de la web, puede configurar parámetros que incluyen parámetros de red, parámetros de video y parámetros independientes; y también puede mantener y actualizar el sistema.

Iniciar sesión

Debe establecer una contraseña y una dirección de correo electrónico antes de iniciar sesión en la web por primera vez. La contraseña que establezca se utiliza para iniciar sesión en la web y el correo electrónico se utiliza para recuperar contraseñas.

Paso 1 Abra el navegador web IE, introduzca la dirección IP (192.168.1.108 de forma predeterminada) del independiente en la barra de direcciones y luego presione Entrar.

Figura 4-1 Inicio de sesión



Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre de usuario predeterminado del administrador es admin, y la contraseña es la contraseña de inicio de sesión después de inicializar el sistema independiente. Modifique la contraseña de administrador con regularidad y consérvela correctamente por motivos de seguridad.
- Si olvida la contraseña de inicio de sesión de administrador, puede hacer clic en **¿Contraseña olvidada?** para restablecerlo. Consulte el manual de usuario.

Paso 3 Haga clic en **Iniciar sesión.**

Se muestra la página de inicio de la web.

5 Funcionamiento del teléfono móvil

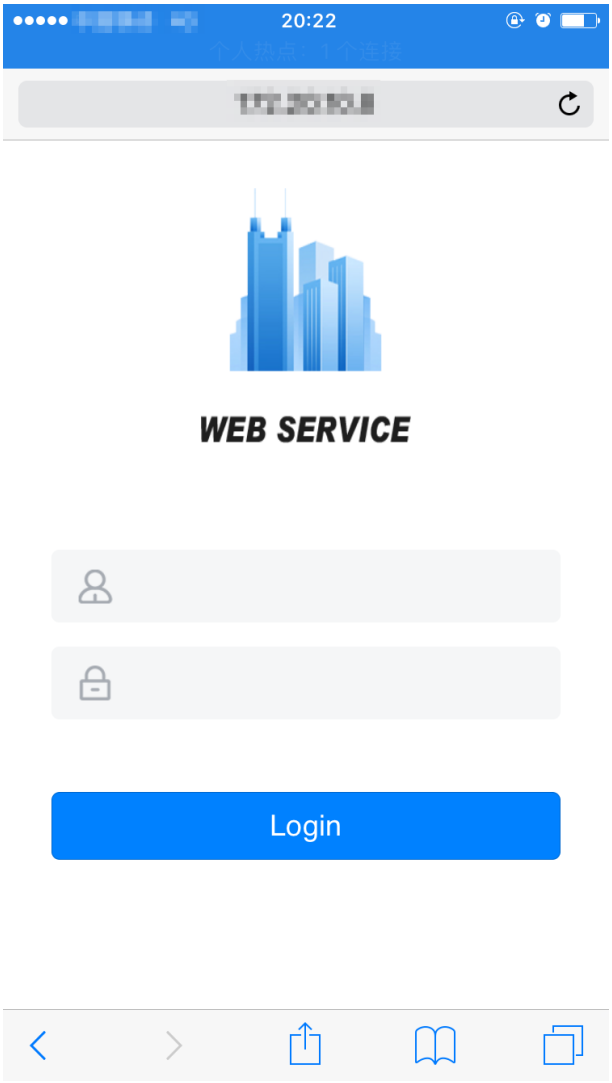
El autónomo se puede configurar y operar en el teléfono móvil. A través del teléfono móvil, puede configurar parámetros, incluidos parámetros de red, parámetros de video y parámetros independientes; y también puede mantener y actualizar el sistema.

Iniciar sesión

Paso 1 Conecte el dispositivo y el teléfono móvil a la misma red.

Paso 2 Abra el navegador en el teléfono móvil, introduzca la dirección IP (se muestra en la Interfaz Wi-Fi, y 192.168.1.108 de forma predeterminada) del independiente en la barra de direcciones, y luego presione Entrar.

Figura 5-1 Inicio de sesión



Paso 3 Introduzca el nombre de usuario y la contraseña.

El nombre de usuario predeterminado del administrador es admin, y la contraseña es la contraseña de inicio de sesión después de inicializar el sistema independiente. Modifique la contraseña de administrador con regularidad y consérvela correctamente por motivos de seguridad.

Paso 4 Haga clic en **Iniciar sesión.**

Se muestra la página de inicio de la web.

Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación, se muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso; No utilice
- caracteres continuos, como 123, abc, etc .; No utilice caracteres superpuestos, como 111,
- aaa, etc .;

2. Actualice el firmware y el software cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su equipo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el equipo está conectado a la red pública, se recomienda habilitar la función de “búsqueda automática de actualizaciones” para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.

- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión con la contraseña incorrecta varias veces, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio en cualquier conjunto de números entre 1024 ~ 65535, reduciendo el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6. **Habilitar HTTPS**

   Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7. **Habilitar lista blanca**

   Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. **Enlace de dirección MAC**

   Le recomendamos que vincule la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

9. **Asignar cuentas y privilegios de forma razonable**

   De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

10. **Deshabilite los servicios innecesarios y elija modos seguros**

    Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir riesgos.

    Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

    - SNMP: elija SNMP v3 y configure contraseñas de autenticación y de cifrado seguras.
    - SMTP: elija TLS para acceder al servidor de buzones de correo. FTP: elija
    - SFTP y configure contraseñas seguras.
    - Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

11. **Transmisión encriptada de audio y video**

    Si su contenido de datos de audio y video es muy importante o sensible, le recomendamos que utilice la función de transmisión encriptada, para reducir el riesgo de robo de datos de audio y video durante la transmisión.

    Recordatorio: la transmisión encriptada provocará cierta pérdida en la eficiencia de transmisión.

12. **Auditoría segura**

    - Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.
    - Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. **Registro de red**

    Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda que habilite la función de registro de red para asegurarse de que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

14. **Construya un entorno de red seguro**

    Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

    - Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
    - La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, es

sugirió utilizar VLAN, red GAP y otras tecnologías para particionar la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Se recomienda que habilite el firewall de su dispositivo o la función de lista negra y lista blanca para reducir el riesgo de que su dispositivo sea atacado.